

REMARKS

In accordance with the foregoing, claims 1, 37 and 40 are amended to clarify the claimed subject matter. No new matter is added. Claims 1-4, 6-24, and 26-41 are pending and under consideration.

Applicants respectfully request entry of this amendment under 37 CFR §1.116 because the amendments of claims 1, 37 and 40 should not entail any further search by the Examiner since no new features are being added or no new issues are being raised

INTERVIEW WITH THE EXAMINER

Applicant's representative wishes to thank the Examiner for the courtesy of an interview granted to Applicant's representative on March 9, 2009, at which time the outstanding issues in this case were discussed. Arguments similar to the ones developed hereinafter were presented and the Examiner indicated that in light of the arguments, he would reconsider the outstanding grounds for rejection upon formal submission of a response.

CLAIM REJECTIONS UNDER 35 U.S.C. §102

Claims 1-4, 6-24, and 26-41 are rejected under 35 U.S.C. §102(e) as allegedly being anticipated by newly cited U.S. Patent No. 6487646 to Adams et al. (hereinafter "Adams").

Independent claim 1 is directed to an information reproducing apparatus including (1) a hardware secure module, (2) a memory, (3) a falsification checking unit and (4) a processor. According to claim 1, the hardware secure module stores information that is not accessible from outside (i.e., a tamper resistant module structure), and the memory can be read using a direct access method without using an operating system. The falsification checking unit "reads the secure software from the memory by direct access without using an operating system, compares the secure software with the information in the hardware secure module, and checks whether the secure software is falsified based on a result of the comparison." The processor "executes the secure software when a result of the check by the falsification checking unit is that the secure software is not falsified."

Adams discloses an apparatus and a method for restricting access to a data storage device of a computer by other computers that prevents unauthorized use, reproduction, and distribution of stored data even when the data storage device is stolen from the computer (see col. 1, lines 7-61 of Adams). In a computer system 50 (see Fig. 2 of Adams), a data storage

device 10 has a data storage media 20 including a key storage area 24 adapted to store a first code and a second code, a data storage region 22 to receive and store data, and a controller 30. The controller 30 sends a first code read out from the key storage area 24 that is accessible only to the controller 30, to a master module 61 of the computer 60. The master module 61 then calculates a comparison value using the first code and sends the comparison value to the controller 30, which then compares the comparison value with a second code stored in the key storage area 24. If the comparison value does not agree with the second code from the key storage area 24, access to the data storage region 22 is denied (see Fig. 2 and col. 4, line 57 to col. 7, line 67 of Adams). Adams also discloses that as an additional security of the computer system 50, the master module 61 may be maintained inaccessible without a key code from the device manufacturer (col. 5, lines 14-17 of Adams).

The result of the security check according to claim 1 is confirming that a secure software stored in a memory has not been falsified and thus being executed by a processor. In contrast the security check in Adams is not related to stored data, but certifies a module to have access to securely stored data. The ultimate results of the security checks being fundamentally different in Adams versus claim 1, the operations for achieving these different results are not obvious if substantially different as argued below.

The Office Action does not indicate which element in the computer system 50 in Fig. 2 anticipates or render obvious the hardware secure module of claim 1. The controller 30 appears to correspond to the falsification checking unit.

Since the key storage area 24 is accessible only to the controller 30, a person of ordinary skill in the art may consider that the key storage area 24 corresponds to the claimed hardware secure module. However, the key storage area 24 in Adams does not store "information related to secure software", but stores a pair of codes, the first code and the second code, that do not appear to have any direct relationship with a secure software or data stored in the data storage region 22. In contrast, according to claim 1, the hardware secure module stores information related to secure software stored in the memory.

Thus, the Office Action fails to put forth a *prima facie* case that the "hardware secure module having a tamper resistant module structure and storing information related to secure software" of the information reproducing apparatus in claim 1 is anticipated or rendered obvious by the prior art.

Further the Office Action takes the position that the master module 61 of the computer system 50 in Fig. 2 of Adams corresponds to the claimed "memory that stores the secure

software." However, nothing indicates that the security check in Adams is related to software stored in the master module 61 or that access and use of the software stored in the master module 61 depends on a positive result of a security check performed by the controller 30.

Relative to the falsification checking unit of claim 1, the Office Action indicates steps 150 and 152 in Fig. 5 of Adams. Fig. 5 of Adams is a flow chart of a method of unlocking a data storage device 10, which has a controller 30, a data region 22 and a key storage area 24 (see col. 2 lines 53-54 and Fig. 2). Steps 150 and 152 in Fig. 5 are operations carried out by the controller 30 in Fig. 2 (see col. 7, lines 9-15 of Adams). However, the controller 30 does not "[read] secure software from the memory by direct access without using an operating system." First (step 146), the controller 30 reads a first code and sends the value to the computer 60 (see col. 7, line 3 of Adams). The computer calculates a comparison value using the first code and sends the calculated comparison value back to the controller 30 (see step 148, col. 7, lines 3-9). Note that Adams does not teach or suggest any direct access reading operation. The controller 30 compares the comparison value with a second code that corresponds to the value of the first code.

If for the sake of argument, one considers that the first code corresponds to the information related to secure software and the second code corresponds to the secure software, Adams fails to anticipate claim 1 because the first and second codes are both stored in the same location, the key storage area 24. In contrast according to claim 1, the information related to secure software is stored in a hardware secure module having a tamper resistant module structure (that is not accessible from outside), while the secure software is stored in the memory.

Thus, the controller 30 does not correspond to the falsification checking unit of claim 1 because fails (a) to "[read] the secure software **from the memory by direct access without using an operating system**" and (b) to "[compare] the secure software **with the information in the hardware secure module.**"

Further the Office Action alleges that step 154 in Fig. 5 of Adams (which is the operation carried out by the controller 30 in Fig. 2, according to the description at column 7, lines 9 to 15) and the disclosure at column 5, lines 4 to 11 (which describes the operation carried out by the master module 61) anticipate the claimed "processor that executes secure software". If one assumes this allegation being true, then the master module 61 in Fig. 2 of Adams corresponds to BOTH the claimed "memory that stores the secure software" AND "processor that executes secure software", and that controller 30 of Adams to BOTH the claimed "falsification checking unit" AND (again) "processor that executes secure software".

It is unclear which description in Adams actually corresponds to the claimed "a hardware secure module having a tamper resistant module structure and storing information related to secure software". In fact, Adams is silent with respect to the claimed "hardware secure module having a tamper resistant module structure and storing information related to secure software". Therefore, Adams cannot teach that the controller 30 alleged to correspond to the claimed "falsification checking unit" being "loaded on the hardware secure module".

Further, Adams fails to teach that the controller 30 "reads the secure software ... by direct access without using an operating system" from the master module 61 alleged to correspond to the claimed "memory". On the contrary, Adams describes that the computer 60 and the controller 30 are accessible to each other via BIOS (column 3, lines 11 to 16). Furthermore, Adams fails to teach that the controller 30 "compares the secure software with the information in the hardware secure module, and checks whether the secure software is falsified based on a result of the comparison" and that the master module 61 and/or the controller 30 "executes the secure software, when a result of the check by the falsification checking unit is that the secure software is not falsified".

Therefore, since Adams does not anticipate all the features recited in claim 1, claim 1 and claims 2-4 and 6-19 depending from claim 1 patentably distinguish over Adams.

In view of the above discussion, independent claim 20 patentably distinguishes over the prior art at least by reciting:

- **reading secure software stored in a memory using direct access method without using an operating system, by a hardware secure module having a tamper resistant module structure which stores information related to the secure software;**
- **checking falsification by comparing the secure software with the information, and determining whether the secure software is falsified based on a result of the comparison. (Emphasis ours related to the above discussed features NOT anticipated by Adams.)**

Independent claim 21 and claims 22-24 and 26-39 depending from claim 21 patentably distinguish over the prior art at least because the following features recited in claim 21 are not anticipated by Adams:

- hardware secure module [...] having a **tamper resistant module structure;**
- a reading unit **that reads a secure software from a memory mounted to the**

information reproducing apparatus by direct access without using an operating system; and

- a falsification checking unit that **compares the secure software with information related to the secure software stored in the hardware secure module**, and checks a falsification of the secure software based on a result of the comparison.

Independent claim 40 patentably distinguishes over the prior art at least by reciting:

- **reading secure software stored in a memory using a direct access method and without using an operating system**, by the hardware secure module having a **tamper resistant module structure storing information related to the secure software;**
- **checking falsification by comparing the secure software with the first information**, and determining a falsification of the secure software based on a result of the comparison.

Independent claim 41 patentably distinguishes over the prior art at least by reciting:

- executing **secure software** that is stored in a memory **accessible** to an information reproducing apparatus **using a direct access method**, if **comparison of the secure software with information related to the secure software stored in a hardware secure module having a tamper resistant module structure inaccessible from outside**, indicates that the secure software is not falsified.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

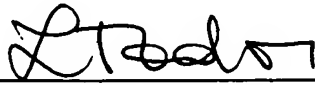
Serial No. 10/629,853

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: April 1, 2009

By: 
Luminita A. Todor
Registration No. 57,639

1201 New York Ave, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501